

#2

REC'D 21 AUG 2003	
WIPO	PCT



**PRIORITY DOCUMENT**  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

**Prioritätsbescheinigung über die Einreichung  
einer Patentanmeldung**

**Aktenzeichen:** 102 36 080.4

**Anmeldetag:** 7. August 2002

**Anmelder/Inhaber:** ROBERT BOSCH GMBH, Stuttgart/DE

**Bezeichnung:** Verfahren und Vorrichtung zur Steuerung von Betriebsabläufen, insbesondere in einem Fahrzeug

**IPC:** G 05 B, G 08 C

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 23. Juli 2003  
Deutsches Patent- und Markenamt  
Der Präsident  
Im Auftrag

Ebert

5 05.08.2002 WRZ/MKU  
Robert Bosch GmbH, 70442 Stuttgart

10 Verfahren und Vorrichtung zur Steuerung von  
Betriebsabläufen, insbesondere in einem Fahrzeug

Die vorliegende Erfindung betrifft ein Verfahren zur  
15 Steuerung und/oder Regelung von Betriebsabläufen,  
insbesondere in einem Fahrzeug. Dabei steht eine  
Funktionseinheit zum Versenden und Empfangen von  
Informationen über mindestens eine Verbindungseinheit mit  
mindestens einem Bussystem in Verbindung. Die  
20 Funktionseinheit wird von einer Überwachungseinheit  
überwacht, das Versenden von Informationen von der  
Funktionseinheit über das mindestens eine Bussystem wird  
durch die Überwachungseinheit unterbunden, falls ein Fehler  
der Funktionseinheit erkannt wird.

Die Erfindung betrifft außerdem eine Vorrichtung zur  
Steuerung und/oder Regelung von Betriebsabläufen,  
insbesondere in einem Fahrzeug. Die Vorrichtung umfasst  
mindestens eine Funktionseinheit, welche zum Versenden und  
30 Empfangen von Informationen über mindestens eine  
Verbindungseinheit mit mindestens einem Bussystem in  
Verbindung steht. Außerdem umfasst die Vorrichtung  
mindestens eine Überwachungseinheit, welche die  
Funktionseinheit überwacht. Die Überwachungseinheit  
35 unterbindet das Versenden von Informationen von der

Funktionseinheit über das mindestens eine Bussystem, falls sie einen Fehler der Funktionseinheit erkennt.

Schließlich betrifft die vorliegende Erfindung auch ein Steuergerät zur Steuerung und/oder Regelung von Betriebsabläufen insbesondere in einem Fahrzeug. Das Steuergerät umfasst eine Funktionseinheit, welche zum Versenden und Empfangen von Informationen über mindestens eine Verbindungseinheit mit mindestens einem Bussystem in Verbindung steht, und eine Überwachungseinheit, welche die Funktionseinheit überwacht. Die Überwachungseinheit unterbindet das Versenden von Informationen von der Funktionseinheit über das mindestens eine Bussystem, falls sie einen Fehler der Funktionseinheit erkennt.

#### Stand der Technik

Aus der DE 198 33 462 A1 ist eine Schaltungsanordnung zur Abkopplung einer elektronischen Einrichtung von einer Datenleitung in einem Kraftfahrzeug bekannt. Über die Datenleitung tauschen die elektronische Einrichtung und mindestens ein weiteres elektrisches System während des Betriebs der elektronischen Einrichtung Informationen aus. Bei der Schaltungsanordnung, bei welcher trotz Ausfall einer an die Datenleitung angeschlossenen elektronischen Einrichtung der Fahrzeugbetrieb aufrechterhalten werden kann, ist die elektronische Einrichtung mit einer Fehlererkennungseinrichtung verbunden. Bei Feststellung eines Fehlers der elektronischen Einrichtung durch die Fehlererkennungseinrichtung wird die elektronische Einrichtung durch die Schaltungsanordnung von der Datenleitung abgekoppelt, wobei die Betriebsfähigkeit des elektrischen Systems aufrechterhalten bleibt.

In der DE 198 33 462 A1 geht es insbesondere um die Überwachung der Datenleitung und um die Erkennung von Fehlern der Datenleitung, welche die Funktionsfähigkeit der an die Datenleitung angeschlossenen elektronischen  
5 Einrichtung beeinträchtigen können. Zum Abkoppeln der elektronischen Einrichtung von der Datenleitung im Fehlerfall ist die Fehlererkennungseinrichtung in die Datenleitung geschaltet und umfasst elektrische  
10 Schaltelemente, um die Datenleitung im Fehlerfall auftrennen zu können. Das setzt jedoch voraus, dass in jeder Datenleitung, mit der die elektronische Einrichtung in Verbindung steht und die im Fehlerfall aufgetrennt werden soll, Schaltelemente angeordnet sein müssen.

15 Aus der DE 100 30 996 A1 ist ein Verfahren und eine Vorrichtung der eingangs genannten Art bekannt. Dort wird vorgeschlagen, dass die Funktionsüberwachung der Funktionseinheit durch die Überwachungseinheit mittels  
20 eines Schaltelements durch die Funktionseinheit aktiviert bzw. deaktiviert werden kann. Das Schaltelement kann bspw. durch Setzen oder Löschen eines Bits realisiert werden. Bei aktivierter Überwachungsfunktion wird die Funktionseinheit von dem Bussystem durch Zugriff getrennt. Dazu steuert die Überwachungseinheit ein weiteres Schaltelement an, durch  
25 das die Verbindung von der Funktionseinheit zu dem Bussystem unterbrochen wird. Als problematisch erweist es sich auch hier, dass ebenfalls gesonderte Schaltelemente in der Verbindung zwischen der Funktionseinheit und dem Bussystem vorgesehen sein müssen, um die Funktionseinheit  
30 im Fehlerfall von dem Bussystem abkoppeln zu können.

Aus dem Stand der Technik sind zudem Überwachungskonzepte für Funktionseinheiten, insbesondere für Kraftfahrsteuergeräte, bekannt, bei denen die  
35 Überwachungseinheit in einem Fehlerfall einen Reset

auslöst. Infolge des Reset fährt die Funktionseinheit erneut hoch und erreicht danach ihren Betriebszustand. Falls der Fehler der Funktionseinheit nach wie vor besteht, erkennt die Überwachungseinheit den Fehler erst in dem Betriebszustand erneut und löst erst dann wieder einen Reset der Funktionseinheit aus. Das Versenden von Informationen von der Funktionseinheit über das Bussystem ist nur kurzzeitig während des Reset-Zustandes unterbunden, da nur in diesem Zustand die Ein-/Ausgangs-Anschlusspositionen (sog. Ports) der Funktionseinheit inaktiv sind. Bei dem bekannten Verfahren kann eine fehlerbehaftete Funktionseinheit also möglicherweise fehlerhaftete Informationen über das Bussystem versenden, obwohl die Überwachungseinheit einen Fehler der Funktionseinheit detektiert hat. Dadurch kann es zu sicherheitsrelevanten Situationen bei der Steuerung der Betriebsabläufe kommen.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, das Versenden von Informationen von der Funktionseinheit über das Bussystem sicher und zuverlässig und auf einfache Weise zu unterbinden.

Zur Lösung dieser Aufgabe schlägt die vorliegende Erfindung ausgehend von dem Verfahren der eingangs genannten Art vor, dass durch die Überwachungseinheit ein Fehlersignal ausgegeben wird, das in Abhängigkeit davon unterschiedliche Werte annimmt, ob ein Fehler der Funktionseinheit erkannt wurde oder nicht, und dass das Fehlersignal an der mindestens einen Verbindungseinheit angelegt und die mindestens eine Verbindungseinheit durch das anliegende Fehlersignal deaktiviert wird, falls ein Fehler der Funktionseinheit erkannt wurde.

## Vorteile der Erfindung

Durch das erfindungsgemäße Verfahren wird bei einem erkannten Fehler der Funktionseinheit von der Überwachungseinheit kein Reset ausgelöst, sondern einfach eine Verbindungseinheit, die zwischen der Funktionseinheit und dem Bussystem angeordnet ist, abgeschaltet. Die Verbindungseinheit ist bspw. als eine Signalverstärkungseinrichtung, insbesondere als eine Bustreiberschaltung des Bussystems (sog. Bus-Driver), ausgebildet. Die Bustreiberschaltung dient insbesondere zur Verstärkung eines von einer Bussteuerung (sog. Bus-Controller) erzeugten Bussignal, bevor es über das Bussystem übertragen wird, sowie zur rückwirkungsfreien Signalanpassung. Erfindungsgemäß bleibt also die Funktionseinheit an sich in einem betriebsfähigen Zustand und kann nach wie vor Informationen erzeugen. Diese Informationen können jedoch nicht mehr über das Bussystem übertragen werden, da die für das Versenden von Informationen erforderliche Verbindungseinheit deaktiviert wurde.

Durch das erfindungsgemäße Verfahren wird eine Beeinträchtigung anderer Funktionseinheiten, die über das Bussystem mit der fehlerbehafteten Funktionseinheit in Verbindung stehen, auf einfache Weise verhindert. Eine fehlerbehaftete Funktionseinheit kann im Fehlerfall somit keine potentiell falschen oder nicht gewünschten Informationen über das Bussystem versenden. Dadurch ergeben sich eigensichere Einzelsysteme in einem Netzwerkverbund.

Besonders vorteilhaft ist, dass das Versenden von Informationen durch die Funktionseinheit ohne den Einsatz zusätzlicher Schaltelemente zwischen der Funktionseinheit und dem Bussystem oder in dem Bussystem selbst sicher und

zuverlässig unterbunden werden kann. Außerdem ist mit der vorliegenden Erfindung das Versenden von Informationen durch die Funktionseinheit dauerhaft unterbunden, was gegenüber einem Reset der Funktionseinheit den Vorteil hat, dass die fehlerhafte Funktionseinheit zu keinem Zeitpunkt Informationen mehr über das Bussystem versenden kann. Sofern es die Fehler der Funktionseinheit zulassen, arbeitet diese noch ganz normal, d. h. sie erzeugt noch Informationen zur Steuerung und/oder Regelung der Betriebsabläufe, wobei diese Informationen allerdings fehlerhaft sein können. Diese Informationen können jedoch nicht über das Bussystem übertragen werden. Durch den weiteren Betrieb der Funktionseinheit ist es möglich, auch in einem Fehlerfall die Funktionseinheit weiterhin zu überwachen und das Versenden von Informationen durch die Funktionseinheit unmittelbar wieder zu erlauben, sobald der Fehler der Funktionseinheit nicht mehr auftritt.

Der Grund für das notwendige Unterbinden des Versendens von Informationen durch die Funktionseinheit im Fehlerfall liegt darin, dass eine fehlerbehaftete Funktionseinheit möglicherweise nicht mehr die Kontrolle über sich selbst und über die korrekte Erzeugung von zu versendenden Informationen hat und sich aufgrund des eigenen Fehlers auch nicht zuverlässig und sicher abschalten kann. Durch eine defekte Funktionseinheit in einem Netzwerkverbund, in dem mehrere Funktionseinheiten über ein Bussystem miteinander in Verbindung stehen, besteht die Gefahr, dass die übrigen empfangenden Funktionseinheiten an dem Bussystem von der fehlerbehafteten sendenden Funktionseinheit fehlerhafte Informationen erhalten und dadurch veranlasst ungewollte Aktionen ausführen. Diese durch fehlerhafte Informationen ausgelösten Aktionen können sich auch sicherheitsrelevant auf die zu steuernden Betriebsabläufe auswirken. Am Beispiel von

Kraftfahrzeugsteuergeräten könnte bspw. ein Steuergerät für die Brennkraftmaschine im Fehlerfall ein Getriebesteuergerät dazu veranlassen, in niedrigere Gänge herunterzuschalten, wodurch das Fahrzeug in einen instabilen Fahrzustand gelangen könnte.

Gemäß einer vorteilhaften Weiterbildung der vorliegenden Erfindung wird vorgeschlagen, dass das Fehlersignal an einen Rücksetzeingang der mindestens einen Verbindungseinheit angelegt wird. Der Rücksetzeingang wird auch als Reset-Eingang bezeichnet. In einem Fehlerfall kann die Verbindungseinheit durch das an dem Rücksetzeingang anliegende Fehlersignal deaktiviert werden.

Gemäß einer bevorzugten Ausführungsform der vorliegenden Erfindung wird vorgeschlagen, dass die Funktionseinheit mit mehreren Bussystemen in Verbindung steht und das Fehlersignal an Verbindungseinheiten mehrerer der Bussysteme angelegt wird. Der Vorteil der vorliegenden Erfindung, dass das Versenden von Informationen durch eine fehlerbehaftete Funktionseinheit ohne den Einsatz zusätzlicher Hardware, wie bspw. zusätzlicher Schaltelemente zum Unterbrechen der Verbindung zwischen fehlerbehafteter Funktionseinheit und Bussystem, sicher und zuverlässig unterbunden werden kann, kommt insbesondere dann zum Tragen, wenn die fehlerbehaftete Funktionseinheit nicht nur mit einem, sondern mit mehreren Bussystemen in Verbindung steht, über die Informationen an andere Funktionseinheiten versandt werden können. Bei allen Bussystemen, die an die fehlerbehaftete Funktionseinheit angeschlossen sind und die in einem Fehlerfall deaktiviert werden sollen, ist das Fehlersignal der Überwachungseinheit an die Verbindungseinheiten geführt. Bussysteme, die nur zur Übertragung von Informationen von nicht sicherheitsrelevanten Betriebsabläufen (z. B. von



Komfortfunktionen) dienen, müssen in einem Fehlerfall der Funktionseinheit nicht unbedingt abgeschaltet werden.

5 Des weiteren wird vorgeschlagen, dass das Fehlersignal an Endstufen von Komponenten angelegt wird, deren Betriebsabläufe von der fehlerbehafteten Funktionseinheit gesteuert bzw. geregelt werden. Diese Komponenten sind bspw. Endstufen von Zündung, Einspritzung und/oder Drosselklappe einer Brennkraftmaschine. Ziel dieser  
10 Maßnahme ist es, die Brennkraftmaschine im Falle eines Fehlers der steuernden bzw. regelnden Funktionseinheit sicher zum Stillstand zu bringen.

15 Als besonders vorteilhaft wird vorgeschlagen, dass nach dem Erkennen eines Fehlers der Funktionseinheit die Funktionseinheit von der Überwachungseinheit weiter überwacht wird und die mindestens eine Verbindungseinheit wieder aktiviert wird, falls eine ordnungsgemäße Funktion der Funktionseinheit erkannt wurde. Diese erneute  
20 Aktivierung der Verbindungseinheiten ist bei der vorliegenden Erfindung jederzeit möglich. Beim Stand der Technik, wo in einem Fehlerfall ein Reset der fehlerbehafteten Funktionseinheit ausgeführt wird, könnte eine ordnungsgemäße Funktion der Funktionseinheit lediglich im Anschluss an den Reset und das Hochfahren der Funktionseinheit erkannt werden. Mit der vorliegenden Erfindung kann somit nicht nur die Sicherheit eines Netzwerkverbundes, welcher mehrere Funktionseinheiten umfasst, die über ein Bussystem miteinander in Verbindung  
30 stehen, sondern auch die Verfügbarkeit des Netzwerkverbundes verbessert werden, da die ordnungsgemäße Funktion einer Funktionseinheit besonders schnell erkannt werden kann.

35 Als eine weitere Lösung der Aufgabe der vorliegenden

Erfindung wird ausgehend von der Vorrichtung der eingangs genannten Art vorgeschlagen, dass die Überwachungseinheit Mittel zum Bilden und Ausgeben eines Fehlersignals aufweist, das in Abhängigkeit davon unterschiedliche Werte annimmt, ob die Überwachungseinheit einen Fehler der Funktionseinheit erkannt hat oder nicht, und dass das Fehlersignal an die mindestens eine Verbindungseinheit geführt ist und die mindestens eine Verbindungseinheit durch das anliegende Fehlersignal deaktivierbar ist, falls ein Fehler der Funktionseinheit erkannt wurde. Die Vorrichtung entspricht bspw. einem Netzwerkverbund, der mehrere Funktionseinheiten umfasst, die über ein Bussystem miteinander in Verbindung stehen.

Gemäß einer vorteilhaften Weiterbildung der vorliegenden Erfindung wird vorgeschlagen, dass das Fehlersignal an einen Enable/Disable-Eingang der mindestens einen Verbindungseinheit geführt ist. Alternativ wird vorgeschlagen, dass das Fehlersignal an einen Reset-Eingang der mindestens einen Verbindungseinheit geführt ist.

Vorteilhafterweise umfasst die Vorrichtung mehrere Funktionseinheiten, die über ein Bussystem miteinander in Verbindung stehen, und mindestens eine Überwachungseinheit, wobei die Überwachungseinheit das Versenden von Informationen von einer Funktionseinheit über das mindestens eine Bussystem unterbindet, falls die Überwachungseinheit einen Fehler dieser Funktionseinheit erkannt hat. Eine solche Vorrichtung entspricht dem in Kraftfahrzeugen in letzter Zeit zunehmend eingesetzten sog. Mehr-Steuergeräte-Konzept, bei dem zur Steigerung der Rechenleistung mehrere Steuergeräte parallel zueinander eingesetzt werden, wobei die einzelnen Steuergerät jeweils einen bestimmten Teil der Betriebsabläufe steuert. So wird bspw. bei einem Zwei-Steuergeräte-Konzept zur Steuerung

einer 8-zyindrigen Brennkraftmaschine ein erstes Steuergerät zur Steuerung von vier der Zylinder und ein zweites Steuergerät zur Steuerung der übrigen vier Zylinder eingesetzt. Die beiden Steuergeräte stehen über ein  
5 Bussystem miteinander in Verbindung. Informationen über den Betriebszustand der Brennkraftmaschine oder des Kraftfahrzeugs werden lediglich dem ersten Steuergerät zugeführt, welches die Informationen dann über das Bussystem an das zweite Steuergerät weiterleitet. Falls die  
10 Überwachungseinheit des ersten Steuergerätes einen Fehler des Steuergerätes erkennt, deaktiviert diese die Verbindungseinheit des Bussystems zu dem zweiten Steuergerät, um zu verhindern, dass das erste Steuergerät fehlerhafte Informationen an das zweite Steuergerät  
15 versendet und das zweite Steuergerät die übrigen vier Zylinder der Brennkraftmaschine falsch ansteuert und sich möglicherweise sogar eine sicherheitsrelevante Situation ergeben könnte.

20 Schließlich wird als noch eine weitere Lösung der Aufgabe der vorliegenden Erfindung ausgehend von dem Steuergerät der eingangs genannten Art vorgeschlagen, dass die Überwachungseinheit Mittel zum Bilden und Ausgeben eines Fehlersignals aufweist, das in Abhängigkeit davon  
25 unterschiedliche Werte annimmt, ob die Überwachungseinheit einen Fehler der Funktionseinheit erkannt hat oder nicht, und dass das Fehlersignal an die mindestens eine Verbindungseinheit geführt ist und die mindestens eine Verbindungseinheit durch das anliegende Fehlersignal  
30 deaktivierbar ist, falls ein Fehler der Funktionseinheit erkannt wurde.

## Zeichnungen

Weitere Merkmale, Anwendungsmöglichkeiten und Vorteile der  
5 Erfindung ergeben sich aus der nachfolgenden Beschreibung  
von Ausführungsbeispielen der Erfindung, die in den  
Zeichnungen dargestellt sind. Dabei bilden alle  
beschriebenen oder dargestellten Merkmale für sich oder in  
beliebiger Kombination den Gegenstand der Erfindung,  
10 unabhängig von ihrer Zusammenfassung in den  
Patentansprüchen oder deren Rückbeziehung sowie unabhängig  
von ihrer Formulierung bzw. Darstellung in der Beschreibung  
bzw. in den Zeichnungen. Es zeigen:

15 Figur 1 ein erfindungsgemäßes Steuergerät gemäß einer  
bevorzugten Ausführungsform;

Figur 2 eine erfindungsgemäße Vorrichtung umfassend zwei  
erfindungsgemäße Steuergeräte, die über ein  
20 Bussystem miteinander in Verbindung stehen; und

Figur 3 Verläufe von verschiedenen Zuständen und Signalen  
eines aus dem Stand der Technik bekannten  
Steuergerätes (Figuren 3b bis 3d) im Vergleich zu  
dem erfindungsgemäßen Steuergerät (Figuren 3e und  
25 3f).

## Beschreibung der Ausführungsbeispiele

30

In Fig. 1 ist ein erfindungsgemäßes Steuergerät SG in  
seiner Gesamtheit mit dem Bezugszeichen 1 bezeichnet. Das  
Steuergerät 1 dient bspw. zur Steuerung und/oder Regelung  
von Betriebsabläufen in einem Kraftfahrzeug. Nachfolgend  
35 wird bspw. auf ein Steuergerät 1 zur Steuerung von

Betriebsabläufen in einer Brennkraftmaschine eines Kraftfahrzeuges näher eingegangen. Die Erfindung ist jedoch generell anwendbar auf alle Arten von Steuergeräten SG, bspw. für eine Getriebesteuerung, eine Fahrdynamikregelung, eine Antriebsschlupfregelung (ASR), eine automatische Abstandsregelung (EDC; Electronic Distance Control), eine adaptive Fahrzeuggeschwindigkeitsregelung (ACC; Adaptive Cruise Control) etc., die über ein Bussystem 2 zu einem Steuergeräteverbund miteinander in Verbindung stehen und über das Bussystem 2 untereinander Informationen austauschen. Das Bussystem 2 ist bspw. als ein CAN (Controller Area Network) ausgebildet.

Das Steuergerät 1 umfasst einen Funktionsrechner FR 3, der bspw. als ein Mikroprozessor oder als ein Mikrocontroller ausgebildet ist. Auf dem Funktionsrechner 3 ist ein Computerprogramm ablauffähig, das zur Erfüllung der Steuerungs- und/oder Regelungsfunktion des Steuergerätes 1 dient. Der Funktionsrechner 3 steht zum Versenden und Empfangen von Informationen über eine Verbindungseinheit 4 mit dem Bussystem 2 in Verbindung. Die Verbindungseinheit 4 ist als eine Hardware-Schnittstelle zwischen einem Controller und einem externen Steuergeräteübertragungsbus mit Signalverstärkungseinrichtung, insbesondere als eine Bustreiberschaltung, z. B. als ein CAN-Treiber für ein CAN-Bussystem, ausgebildet. Der CAN-Treiber 4 wird auch als CAN-Driver bezeichnet.

Die in dem Funktionsrechner 3 im Rahmen der Abarbeitung des Computerprogramms zur Erfüllung der Steuerungs- und/oder Regelungsfunktion des Steuergerätes 1 erzeugten Informationen werden über einen Datenbus 5 zunächst an eine CAN-Steuerung 6 übertragen, die auch als CAN-Controller bezeichnet wird. In der CAN-Steuerung 6 werden die von dem Funktionsrechner 3 erzeugten Informationen in eine dem CAN-

Protokoll entsprechende Form gebracht und für die Übertragung über das CAN-Bussystem 2 vorbereitet. Vor der Übertragung der aufbereiteten Informationen müssen die Signale noch an die elektrischen Eigenschaften auf dem CAN-Bus angepasst werden. Dazu werden die aufbereiteten Informationen über eine zwei-Draht-Datenleitung 7 von der CAN-Steuerung 6 an den CAN-Treiber 4 übertragen, der die Signale auf das CAN-Bussystem 2 legt.

Dem Funktionsrechner 3 ist eine unabhängige Hardware zur Funktionsüberwachung des Funktionsrechners 3 zugeordnet. Die unabhängige Hardware wird als Überwachungsmodul UM 8 bezeichnet. Das Überwachungsmodul 8 stellt dem Funktionsrechner 3 zyklisch verschiedene Fragen, die in dem Funktionsrechner 3 umfangreiche Kontrollmechanismen, wie bspw. Programmablaufkontrollen oder Befehlstests, durchlaufen und ein Ergebnis bilden. Das Ergebnis wird als Antwort auf die Frage dem Überwachungsmodul 8 zurück übertragen. Ein fehlerfrei arbeitender Funktionsrechner 3 liefert die richtige Antwort innerhalb eines vorgebbaren Zeitfensters zurück. Das Überwachungsmodul 8 stellt durch Auswerten der Antwort fest, ob ein Fehler des Funktionsrechners 3 vorliegt oder nicht. Das beschriebene Überwachungskonzept des Funktionsrechners 3 durch das Überwachungsmodul 8 wird auch als Frage-Antwort-Kommunikation bezeichnet. Die Kommunikation zwischen dem Überwachungsmodul 8 und dem Funktionsrechner 2 erfolgt über eine SPI (Serial Parallel Interface)-Schnittstelle 9.

Durch Auswerten der Antwort des Funktionsrechners 3 wird in dem Überwachungsmodul 8 ein Fehlersignal WDA generiert, das in Abhängigkeit davon unterschiedliche Werte annimmt, ob ein Fehler des Funktionsrechners 3 erkannt wurde oder nicht. Vorzugsweise wird ein Fehlerzähler inkrementiert, falls ein Fehler des Funktionsrechners 3 erkannt wurde.

Erst wenn der Fehlerzähler einen Schwellenwert überschritten hat, wird das Fehlersignal WDA ausgegeben. Das Fehlersignal WDA wird über eine Signalleitung 10 an Endstufen E1 bis EN von Kraftfahrzeugkomponenten K1 bis Kn, die von dem Steuergerät 1 zur Steuerung und/oder Regelung der Betriebsabläufe angesteuert werden, angelegt. Dies sind bspw. bei einem Kraftfahrzeugsteuergerät 1 zur Steuerung und/oder Regelung einer Brennkraftmaschine die Endstufen für Zündung, Einspritzung und/oder Drosselklappe. Die Ansteuerung der Endstufen E1 bis En mit dem Fehlersignal WDA dient dazu, im Fehlerfall die Brennkraftmaschine sicher zum Stillstand zu bringen und sicherheitsrelevante Situationen zu vermeiden.

Erfindungsgemäß wird das Fehlersignal WDA außerdem an einen Reset-Eingang RST des CAN-Treibers 4 angelegt. Der CAN-Treiber 4 wird durch das anliegende Fehlersignal WDA deaktiviert, falls ein Fehler des Funktionsrechners 3 erkannt wurde. Dadurch wird das Versenden von Informationen durch einen defekten Funktionsrechner 3 über das CAN-Bussystem 2 zuverlässig, wirksam und vor allem dauerhaft für die gesamte Dauer des Fehlers des Funktionsrechners 3 unterbunden. Dadurch wird auch das Versenden möglicherweise fehlerhafter Informationen durch den fehlerbehafteten Funktionsrechner 3 über das CAN-Bussystem 2 an andere Funktionsrechner auf einfache Weise verhindert. Das erfindungsgemäße Steuergerät 1 stellt somit ein eigensicheres Eigensystem in einem Steuergeräteverbund dar. Es erfüllt die Vorschriften an Steuergeräte in einem Steuergeräteverbund, dass nämlich jedes Steuergerät 1 die Verantwortung für die von ihm versendeten Informationen selbst trägt.

Ein weiterer Vorteil der vorliegenden Erfindung besteht darin, dass ein fehlerbehafteter Funktionsrechner 3

weiterhin normal arbeitet und weiterhin - zwar möglicherweise fehlerhafte - Informationen zur Steuerung der Betriebsabläufe ermittelt. Das Überwachungsmodul 8 kann somit auch nach dem Erkennen eines Fehlers des

5 Funktionsrechners 3 die Funktionsfähigkeit des Funktionsrechners 3 weiterhin überwachen. Solange das Überwachungsmodul 8 einen Fehler des Funktionsrechners 3 erkennt, bleibt der CAN-Treiber 4 deaktiviert, damit die von dem fehlerhaften Funktionsrechner 3 ermittelten  
10 fehlerhaften Informationen nicht auf das CAN-Bussystem 2 gelangen und andere Funktionsrechner des Steuergeräteverbundes beeinträchtigen können. Sobald das Überwachungsmodul 8 jedoch eine ordnungsgemäße Funktion des Funktionsrechners 2 erkennt, kann der CAN-Treiber 4 wieder  
15 aktiviert werden, so dass das Steuergerät 1 wieder ganz normal arbeiten kann. Vorteilhaft bei der vorliegenden Erfindung ist es, dass eine ordnungsgemäße Funktion des Funktionsrechners 3 ohne lange Zeitverzögerung erkannt werden kann.

20 Noch ein Vorteil der Erfindung ist darin zu sehen, dass das Versenden von Informationen durch einen fehlerbehafteten Funktionsrechner 3 auf einfache Weise und ohne zusätzliche Hardware, bspw. ohne zusätzliche Schaltelemente, die in das CAN-Bussystem 2 eingebracht werden und im Fehlerfall geöffnet werden, um den Funktionsrechner 3 von dem CAN-Bussystem 2 zu trennen, unterbunden werden kann.

30 In Fig. 2 ist ein Mehr-Steuergeräte-Konzept, genauer gesagt ein Zwei-Steuergeräte-Konzept, dargestellt, bei dem zwei Steuergeräte SG1, SG2 zur Steuerung bestimmter Betriebsabläufe eingesetzt werden. In dem dargestellten Ausführungsbeispiel sind die zwei Steuergeräte SG1, SG2 zur  
35 Steuerung der Betriebsabläufe in einer 12-zyklindrigen Brennkraftmaschine BM 11 eingesetzt. Dabei steuert das



erste Steuergerät SG1 die ersten sechs Zylinder ZYL 12 und das zweite Steuergerät SG2 die übrigen sechs Zylinder ZYL 13. Das erste Steuergerät SG1 erhält Informationen S über den Fahrerwunsch (Stellung des Gaspedals) und/oder über den Betriebszustand der Brennkraftmaschine 11 und des Kraftfahrzeugs von entsprechenden Sensoren. Die beiden Steuergeräte SG1 und SG2 sind über ein CAN-Bussystem 2 miteinander verbunden. Das zweite Steuergerät SG2 erhält über das CAN-Bussystem 2 Sollwertvorgaben (z.B. den Fahrerwunsch) von dem ersten Steuergerät SG1. Um zu verhindern, dass bei einem Fehler des Funktionsrechners FR1 des ersten Steuergerätes SG1 fehlerhafte Sollwertvorgaben an das zweite Steuergerät SG2 übermittelt werden, wird erfindungsgemäß das Versenden von Informationen durch den Funktionsrechner FR1 über das CAN-Bussystem 2 durch die Überwachungseinheit ÜM1 unterbunden. Dazu wird das Fehlersignal WDA des Überwachungsmoduls ÜM1 an einen Reset-Eingang RST des CAN-Treibers 4 angelegt.

Anhand der ausbleibenden Datenübertragung (Nachrichtenunterbrechung bzw. fehlende Aktualisierung) kann das Steuergerät SG2 einen Defekt im SG1 erkennen und entsprechende Ersatzmaßnahmen oder Fehlerreaktionen im SG2 aktivieren.

In den Figuren 3a bis 3f sind die Verläufe verschiedener Steuergerätezustände und Steuergerätegrößen über die Zeit  $t$  dargestellt. Insbesondere ist in Fig. 3a der Stand eines Fehlerzählers des Überwachungsmoduls 8 dargestellt. Dieser steigt am Anfang von Null bis über einen Schwellenwert SW an. Sobald der Fehlerzähler den Schwellenwert SW übersteigt, wird zum Zeitpunkt  $t_1$  eine Fehlerreaktion ausgelöst. Das bedeutet, dass das Fehlersignal WDA einen entsprechenden Wert annimmt. Als Werte des Fehlersignals WDA kommen insbesondere HIGH oder LOW in Frage.

Die in den Figuren 3b, 3c und 3d dargestellten Verläufe entsprechen dem Stand der Technik. In Fig. 3b ist der Verlauf eines Reset-Signals dargestellt, welches nach dem Stand der Technik von dem Überwachungsmodul ÜM 8 an einen Reset-Eingang des Funktionsrechners FR 3 angelegt wird. Zum Zeitpunkt  $t_1$  wird die Fehlerreaktion ausgelöst, die beim Stand der Technik darin besteht, einen Reset des Funktionsrechners FR 3 auszulösen. In Fig. 3c ist der Verlauf einer Größe "CAN-Signal freigegeben" dargestellt. Das Signal hat die Werte „frei“ oder „gesperrt“. Fig. 3c kann entnommen werden, dass das CAN-Signal nur während der Dauer des Reset ( $RST = 1$  in Fig. 3b) gesperrt ist und ansonsten frei ist. Solange das CAN-Signal freigegeben ist, kann selbst ein fehlerbehafteter Funktionsrechner FR 3 möglicherweise fehlerhafte Informationen über das CAN-Bussystem 2 übertragen. Dies kann unter Umständen fehlerhafte Reaktionen anderer Funktionsrechner FR des Steuergeräteverbundes auslösen.

In Fig. 3d sind verschiedene Zustände des aus dem Stand der Technik bekannten Steuergeräts SG dargestellt. Vor dem Auslösen der Fehlerreaktion zum Zeitpunkt  $t_1$  durchläuft das Steuergerät SG ein ganz normales Fahrprogramm A. Danach schließt sich nach dem Zeitpunkt  $t_1$  ein Reset-Zustand B an. Im Anschluss daran durchläuft das Steuergerät SG eine Initialisierungsphase C und wechselt danach wiederum in das normale Fahrprogramm A. Während des Fahrprogramms A führt das Überwachungsmodul ÜM eine Frage-Antwort-Kommunikation mit dem zu überwachenden Funktionsrechner FR durch und erkennt an einem Zeitpunkt  $t_2$ , dass der Fehler des Funktionsrechners FR immer noch vorliegt. Danach werden wiederum die vorbeschriebenen Zustände Reset B, Initialisierung C und Fahrprogramm A mit Frage-Antwort-Kommunikation D durchlaufen.

In den Figuren 3e und 3f sind die Signal- und Zustandsverläufe des erfindungsgemäßen Steuergeräts 1 dargestellt. Anhand der Fig. 3e ist deutlich zu erkennen, dass das CAN-Signal unmittelbar nach der Fehlerreaktion zum Zeitpunkt  $t_1$  für die Dauer des Fehlers gesperrt ist. Der Funktionsrechner 3 befindet sich nach der Fehlerreaktion in einem ganz normalen Fahrprogramm A, währenddessen eine Frage-Antwort-Kommunikation D zyklisch ausgeführt wird und die Endstufen über das WDA-Signal sich im deaktivierten Zustand befinden (E). Allerdings werden die von dem Funktionsrechner 3 ermittelten Informationen nicht über das CAN-Bussystem 2 übertragen, da der CAN-Treiber 4 deaktiviert ist und das CAN-Signal somit gesperrt ist. Bei der vorliegenden Erfindung befindet sich der Funktionsrechner 3 im Fehlerfall niemals in einer Situation in der nicht die Funktionsfähigkeit des Funktionsrechners 3 durch eine Frage-Antwort-Kommunikation überprüft werden könnte. Dagegen kann beim Stand der Technik im Fehlerfall eine Überprüfung der Funktionsfähigkeit des Funktionsrechners 3 nicht während der Zustände Reset B und Initialisierung C erfolgen. Dadurch kann die ordnungsgemäße Funktion des Funktionsrechners 3 bei der vorliegenden Erfindung früher als beim Stand der Technik erkannt werden.

5 05.08.2002 WRZ/MKU  
Robert Bosch GmbH, 70442 Stuttgart

10 Ansprüche

1. Verfahren zur Steuerung und/oder Regelung von Betriebsabläufen, insbesondere in einem Fahrzeug, wobei eine Funktionseinheit (3) zum Versenden und Empfangen von  
15 Informationen über mindestens eine Verbindungseinheit (4) mit mindestens einem Bussystem (2) in Verbindung steht, die Funktionseinheit (3) von einer Überwachungseinheit (8) überwacht wird und das Versenden von Informationen von der Funktionseinheit (3) über das mindestens eine Bussystem (2)  
20 durch die Überwachungseinheit (8) unterbunden wird, falls ein Fehler der Funktionseinheit (3) erkannt wird, **dadurch gekennzeichnet**, dass durch die Überwachungseinheit (8) ein Fehlersignal (WDA) ausgegeben wird, das in Abhängigkeit davon unterschiedliche Werte annimmt, ob ein Fehler der  
25 Funktionseinheit (3) erkannt wurde oder nicht, und dass das Fehlersignal (WDA) an der mindestens einen Verbindungseinheit (4) angelegt und die mindestens eine Verbindungseinheit (4) durch das anliegende Fehlersignal (WDA) deaktiviert wird, falls ein Fehler der  
30 Funktionseinheit (3) erkannt wurde.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Fehlersignal (WDA) an einen Rücksetzeingang (RST) der mindestens einen Verbindungseinheit (4) angelegt wird.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Funktionseinheit (3) mit mehreren Bussystemen (2) in Verbindung steht und das Fehlersignal (WDA) an Verbindungseinheiten (4) mehrerer der Bussysteme (2) angelegt wird.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass das Fehlersignal (WDA) an Endstufen (E1, ... En) von Komponenten (K1, ... Kn) angelegt wird, deren Betriebsabläufe gesteuert bzw. geregelt werden.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass nach dem Erkennen eines Fehlers der Funktionseinheit (3) die Funktionseinheit (3) von der Überwachungseinheit (8) weiter überwacht wird und die mindestens eine Verbindungseinheit (4) wieder aktiviert wird, falls eine ordnungsgemäße Funktion der Funktionseinheit (3) erkannt wurde. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass nach dem Erkennen eines Fehlers der Funktionseinheit (3) die Funktionseinheit (3) nicht zurückgesetzt wird, weiterhin aktiv ein Computerprogramm abarbeitet, und der Sende- und Empfangsbetrieb von der Überwachungseinheit (8) durch Aktivierung bzw. Deaktivierung der Verbindungseinheit (4) gesteuert wird.

6. Vorrichtung zur Steuerung und/oder Regelung von Betriebsabläufen, insbesondere in einem Fahrzeug, umfassend mindestens eine Funktionseinheit (3), welche zum Versenden und Empfangen von Informationen über mindestens eine Verbindungseinheit (4) mit mindestens einem Bussystem (2) in Verbindung steht, und mindestens eine Überwachungseinheit (8), welche die Funktionseinheit (2) überwacht, wobei die Überwachungseinheit (8) das Versenden von Informationen von der Funktionseinheit (3) über das mindestens eine Bussystem (2) unterbindet, falls sie einen

Fehler der Funktionseinheit (3) erkennt, **dadurch gekennzeichnet**, dass die Überwachungseinheit (8) Mittel zum Bilden und Ausgeben eines Fehlersignals (WDA) aufweist, das in Abhängigkeit davon unterschiedliche Werte annimmt, ob  
5 die Überwachungseinheit (8) einen Fehler der Funktionseinheit (3) erkannt hat oder nicht, und dass das Fehlersignal (WDA) an die mindestens eine Verbindungseinheit (4) geführt ist und die mindestens eine Verbindungseinheit (4) durch das anliegende Fehlersignal  
10 (WDA) deaktivierbar ist, falls ein Fehler der Funktionseinheit (3) erkannt wurde.

7. Vorrichtung nach Anspruch 5, dadurch gekennzeichnet, dass das Fehlersignal (WDA) an einen Enable/Disable-Eingang der mindestens einen Verbindungseinheit (4) geführt ist.

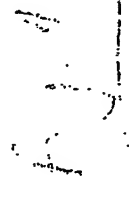
15 8. Vorrichtung nach Anspruch 5, dadurch gekennzeichnet, dass das Fehlersignal (WDA) an einen Rücksetzeingang (RST) der mindestens einen Verbindungseinheit (4) geführt ist.

9. Vorrichtung nach einem der Ansprüche 5 bis 7, dadurch gekennzeichnet, dass die Vorrichtung mehrere  
20 Funktionseinheiten (3), die über ein Bussystem (2) miteinander in Verbindung stehen, und mindestens eine Überwachungseinheit (8) umfasst, wobei die Überwachungseinheit (8) das Versenden von Informationen einer Funktionseinheit (3; FR1) über das mindestens eine  
25 Bussystem (2) unterbindet, falls die Überwachungseinheit (8) einen Fehler dieser Funktionseinheit (3; FR1) erkannt hat.

10. Steuergerät (1) zur Steuerung und/oder Regelung von Betriebsabläufen insbesondere in einem Fahrzeug, umfassend  
30 eine Funktionseinheit (3), welche zum Versenden und Empfangen von Informationen über mindestens eine Verbindungseinheit (4) mit mindestens einem Bussystem (2)

in Verbindung steht, und eine Überwachungseinheit (8),  
welche die Funktionseinheit (3) überwacht, wobei die  
Überwachungseinheit (8) das Versenden von Informationen von  
der Funktionseinheit (3) über das mindestens eine Bussystem  
5 (2) unterbindet, falls sie einen Fehler der  
Funktionseinheit (3) erkennt, **dadurch gekennzeichnet**, dass  
die Überwachungseinheit (8) Mittel zum Bilden und Ausgeben  
eines Fehlersignals (WDA) aufweist, das in Abhängigkeit  
davon unterschiedliche Werte annimmt, ob die  
10 Überwachungseinheit (8) einen Fehler der Funktionseinheit  
(3) erkannt hat oder nicht, und dass das Fehlersignal (WDA)  
an die mindestens eine Verbindungseinheit (4) geführt ist  
und die mindestens eine Verbindungseinheit (4) durch das  
anliegende Fehlersignal (WDA) deaktivierbar ist, falls ein  
15 Fehler der Funktionseinheit (3) erkannt wurde.

11. Steuergerät (SG) nach Anspruch 9, **dadurch**  
gekennzeichnet, dass das Fehlersignal (WDA) an einen  
Rücksetzeingang (RST) der mindestens einen  
Verbindungseinheit (4) geführt ist.





A hand-drawn diagram of a three-strand braid. The strands are labeled 12, 11, and 13 from left to right. The crossings are labeled 11, 12, and 13. The crossings are arranged in a sequence from top to bottom: first a crossing between strands 12 and 11 (labeled 11), then a crossing between strands 11 and 13 (labeled 12), and finally a crossing between strands 12 and 11 (labeled 13).

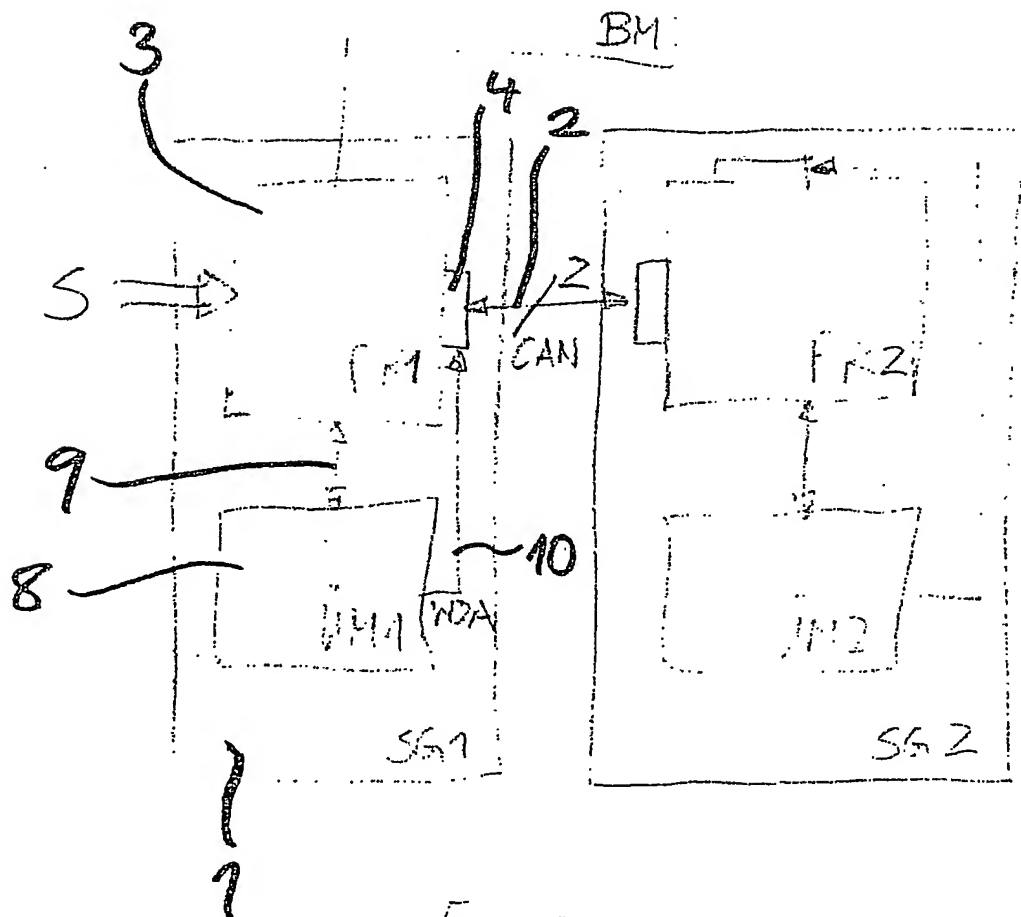
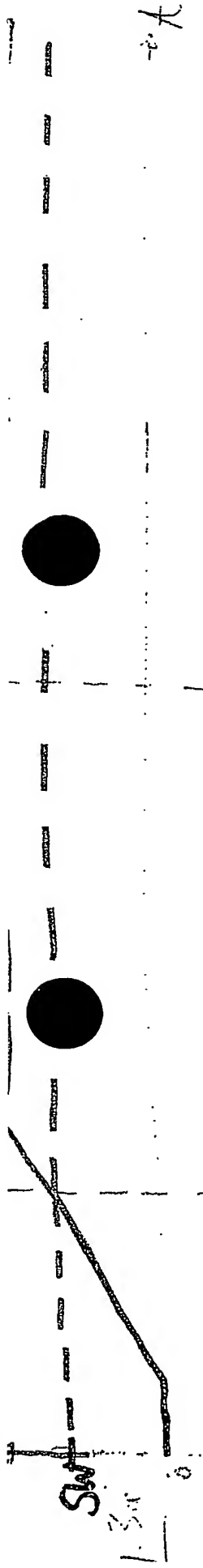


Fig. 2



2.7

RST 1

3b



2.7

CAN A<sub>1</sub> 4/10

1.3µs

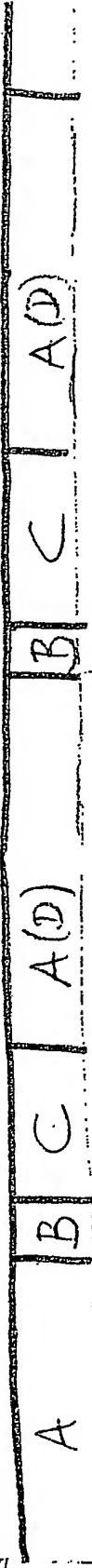


2.7

3/3

Zustand FR

1.3µs



2.7

CAN A<sub>1</sub> 4/10

1.3µs



2.7

Zustand FR

1.3µs



2.7

2.7

2.7

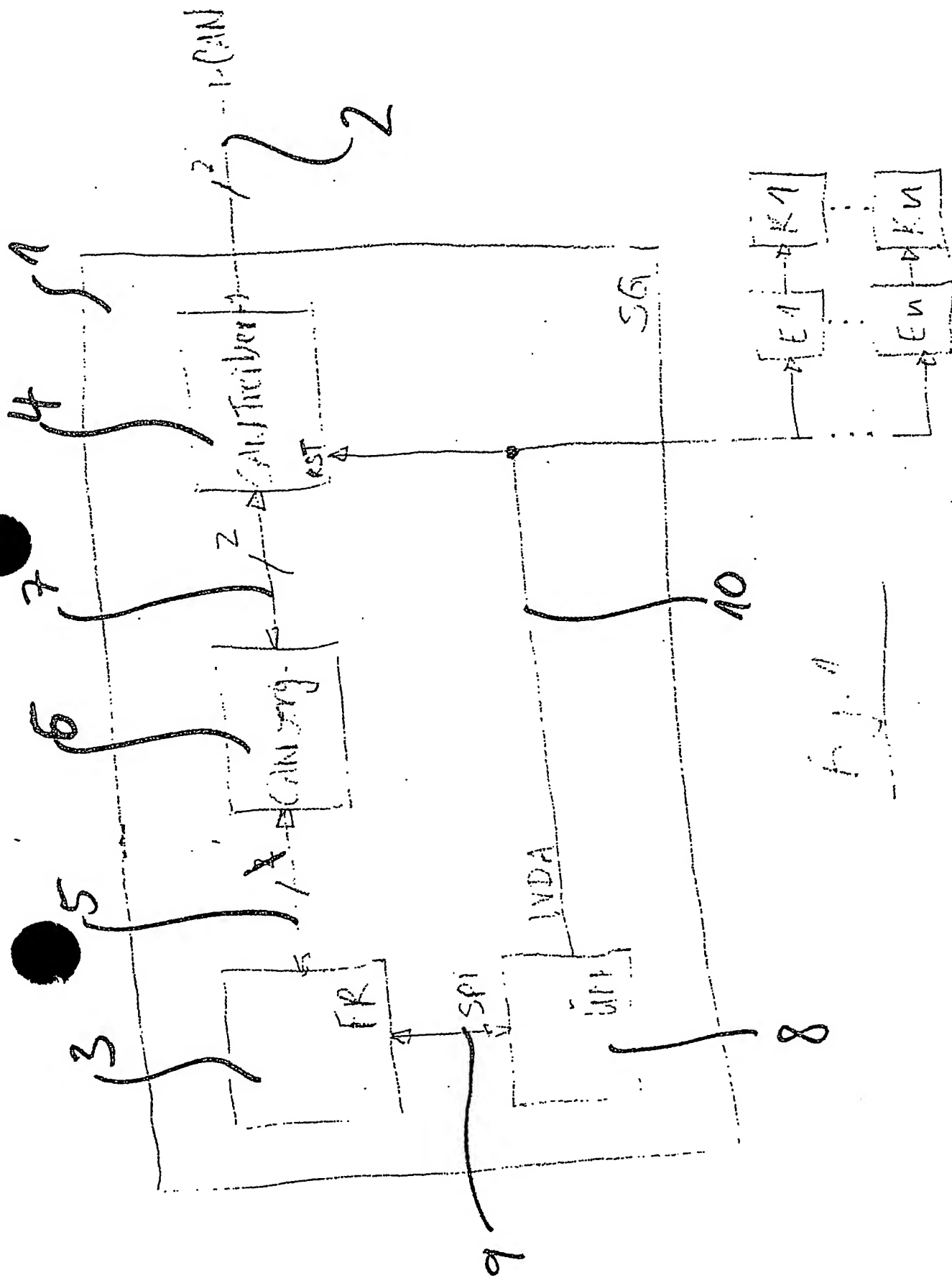
A(D) A(D) (E)

5 05.08.2002 WRZ/MKU  
Robert Bosch GmbH, 70442 Stuttgart

### Zusammenfassung

#### Verfahren und Vorrichtung zur Steuerung von Betriebsabläufen, insbesondere in einem Fahrzeug

15 Die Erfindung betrifft ein Verfahren und eine Vorrichtung zur Steuerung von Betriebsabläufen, insbesondere in einem Fahrzeug. Dabei steht eine Funktionseinheit (3) zum Versenden und Empfangen von Informationen über mindestens eine Verbindungseinheit (4) mit mindestens einem Bussystem (2) in Verbindung. Die Funktionseinheit (3) wird von einer Überwachungseinheit (8) überwacht. Das Versenden von Informationen von der Funktionseinheit (3) über das mindestens eine Bussystem (2) wird durch die Überwachungseinheit (8) unterbunden, falls ein Fehler der Funktionseinheit (3) erkannt wird. Um das Versenden von Informationen durch die Funktionseinheit (8) in einem Fehlerfall auf eine möglichst einfache Weise, aber dennoch sicher und zuverlässig zu unterbinden, wird vorgeschlagen, dass durch die Überwachungseinheit (8) ein Fehlersignal (WDA) ausgegeben wird, das in Abhängigkeit davon unterschiedliche Werte annimmt, ob ein Fehler der Funktionseinheit (3) erkannt wurde oder nicht, und dass das Fehlersignal (WDA) an der mindestens einen Verbindungseinheit (4) angelegt und die mindestens eine Verbindungseinheit (4) durch das anliegende Fehlersignal (WDA) deaktiviert wird, falls ein Fehler der Funktionseinheit (3) erkannt wurde. (Figur 1)



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**